

REMARKS

In this response to the above-identified Office Action, Applicants respectfully request reconsideration in view of the above amendments and following remarks. Claims 1-4 and 8-16 have been amended. No claims have been added or cancelled. Accordingly, claims 1-4 and 8-16 are pending in the application.

Claim Amendments

Applicants have amended Claims 1-4 and 8-16 to clarify that the claims are directed to a method. These and other minor amendments have been made in light of clarifying the claim language, and do not alter the scope of the claim limitations. Applicants respectfully submit that no new matter has been added, and that the amendments are within the scope of Examiner's search.

Claims Rejected Under 35 U.S.C. § 101

Claims 1-32 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicant respectfully disagrees for the following reasons.

The Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility (hereinafter “Guidelines”) as presented in MPEP § 2106 guide the analysis of whether claims constitute § 101 statutory subject matter.

The Guidelines indicate that statutory subject matter 1) must fall within one of the enumerated statutory categories, Guidelines, at § IV(B), and 2) must not fall within one of the judicial exceptions of “abstract ideas, laws of nature, and natural phenomena,” *id.* at § IV(C). However, a *practical application* of an abstract idea, law of nature, or natural phenomenon may be patented. *Id.* at § IV(C)(1). A practical application may be identified by either 1) a physical transformation of an article or physical object to a different state or thing; or 2) the production of a “useful, concrete and tangible result.” *Id.* at § IV(C)(2).

Examiner states that the claims recite “A digital signature scheme based on braid groups conjugacy problem,” allegedly raising “a question as to whether the claims are directed merely to an abstract idea and mathematical algorithm that are not tied to a

technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter.”

As amended, the claims have been clarified to direct the language to a “method.” Hence, Applicants respectfully submit that the subject matter for which protection is sought in the claims is a process, which falls within an enumerated statutory category under 35 U.S.C. § 101. Further, the claimed subject matter is not directed merely toward an “abstract idea and mathematical algorithm,” but rather, is directed to a practical application.

Applicant submits that each of the present claims is directed to a practical application at least because produces a useful, concrete, and tangible result. The focus of this inquiry is “not on whether the steps taken to achieve a particular result are useful, tangible, and concrete, but rather on whether the final result achieved by the claimed invention is ‘useful, tangible, and concrete.’” *Id.* at § IV(C)(2)(2).

Applicants submit that the claimed subject matter is useful, since it is “(i) specific, (ii) substantial and (iii) credible.” *Id.* at § IV(C)(2)(2)(a). The method of claim 1 is a digital signature method based on braid group conjugacy, and it is a method employed to solve a technical problem. The problem to be solved is that of “excess consumption of computer calculation resource in generating big prime number and dividing hack of big number, and the problem of taking excess time to generate key and verify signature due to the increased calculation and data used for CSS to resolve the k-CSP problem in the SCSS,” Specification (as published in Pub. No. 2007/0104322), at ¶ 0017. The claim employs the “exchangeability of the left subgroup and the right subgroup of the braid groups,” Specification, at ¶ 0049, and includes the technical means of “generating a braid b from the right subgroup $RB_{n-l-m}(l)$ at random” in step 3. This results in a corresponding technical advantage of “reduc[ing] the number of braids involved and the number for conjugacy decision” and overcomes the problem of excess consumption of computer calculation resource and the problem of taking excess time to generate key and verify signature, without reducing the security, and therefore, improves the operation efficiency of signature. *See* Specification, at ¶¶ 0049-0050. Thus, the claimed subject matter satisfies the utility requirement of § 101.

Applicants also submit that the claimed subject matter is tangible. The claim “set[s] forth a practical application . . . to produce a real-world result,” as required by the Guidelines.

Id. at § IV(C)(2)(2)(b). For example, the method at least “output[s] message (*M*) and a signature of message (*M*) *Sign(M)*.”

Further, the claimed subject matter is concrete. Applicants submit that the claimed method has “a result that can be substantially repeatable or the process must substantially produce the same result again,” as required by the Guidelines. *Id.* at § IV(C)(2)(2)(c).

The present claims thus produce a “useful, concrete and tangible result” and are therefore directed to a practical application.

For the reasons above, Claim 1 is directed to statutory subject matter under 35 U.S.C. § 101. Accordingly, reconsideration and withdrawal of the subject matter rejection of this claim are requested.

Independent Claim 8, as amended, includes elements similar to those of Claim 1. For at least the reasons discussed above in relation to Claim 1, Applicants submit that Claim 8 is also directed to statutory subject matter under 35 U.S.C. § 101. Accordingly, reconsideration and withdrawal of the subject matter rejection of this claim are requested.

Claims 2-4 and 9-16 depend from Claims 1 and 8, respectively, and include the limitations thereof. Thus, for at least the reasons discussed above in relation to the independent claims, Applicants submit that the dependent claims are also directed to statutory subject matter under 35 U.S.C. § 101. Accordingly, reconsideration and withdrawal of the subject matter rejection of these claims are requested.

Applicants believe that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application; the undersigned can be reached at the telephone number set out below.

The Commissioner is hereby authorized to charge any additional fees due or credit any overpayment to Deposit Account No. 50-2421.

Sincerely,

Dated: September 8, 2008

/David R. Stevens/
David R. Stevens
Reg. No. 38,626

Stevens Law Group
1754 Technology Drive, Suite 226
San Jose, CA 95110
Phone (408) 288-7588
Fax (408) 288-7542